Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 5-8, 11-14, 17-21, 48, 49, 51-54, and 68-79 are pending in the application, claims 68, 73, and 78 being the independent claims. Claims 68, 73, and 78 are sought to be amended. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 103

Kawamura and Cheung

Claims 5-8, 11, 12, 17-21, 48, 49, 51, 52, and 68-79 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,940,975 to Kawamura, et al (Kawamura) in view of Cheung, et al, *Implementation of Pipelined Data Encryption Standard* (Cheung). Applicants respectfully traverse this rejection.

The combination of Karamura and Cheung does not teach or suggest each and every limitation of the amended independent claims 68, 73, and 78. The Office Action acknowledges that Kawamura "fails to explicitly disclose wherein the key scheduler includes a multi-stage pipeline and is further configured to generate a round key each clock cycle after a series of initialization clock cycles." (Office Action, p. 4). However, the Office Action alleges that this feature is disclosed in Chueng. Applicants respectfully disagree.

Cheung describes a piplined architecture for DES. In the fully pipeline architecture, hardware for processing each of the 16 DES rounds is built separately. In this architecture, 16 different inputs can be fed into the pipeline at the same time. (Cheung, III-18). In the compromised pipelined DES, a 4 segment pipline is implemented. (Cheung, III-19). In this architecture, four DES rounds can be processed simultaneously. The compromised pipelined DES loads 4 different inputs for the first four rounds. (Cheung, III-20). Each round also receives a round key. Chueng thus describes the pipelining of cryptographic rounds. Therefore, Cheung does not teach or describe the pipelining of key generation for each individual round.

Thus, Cheung does not teach or suggest

> a key scheduler configured to provide a plurality of keys for cryptographic operation rounds, wherein the key scheduler includes a multi-stage pipeline and is further configured to generate a round key each clock cycle after a series of initialization clock cycles; and
>
> cryptographic round logic, wherein the cryptographic round logic is configured to receive a key from the key scheduler for a current cryptographic round and wherein the cryptographic round logic includes:
>
> means for combining via a first logical operation the key provided by the key scheduler with a first bit sequence to generate a second bit sequence, wherein the first bit sequence is an expansion of the first portion of the data block;

as recited in amended independent claims 68 and 73. Cheung also does not teach or suggest:

> a key scheduler configured to provide a plurality of keys for cryptographic operation rounds, wherein the key scheduler includes a multi-stage pipeline and is further configured to generate a round key each clock cycle after a series of initialization clock cycles; and
>
> cryptographic round logic, wherein the cryptographic round logic is configured to receive a key from the key scheduler for a

> current cryptographic round and wherein the cryptographic round logic includes:
>
> an expansion logic for expanding the first portion of the data block and for generating a first bit sequence having a first bit size;
>
> a first XOR logic for performing a first XOR operation of a first key provided by the key scheduler and the first bit sequence and for generating a second bit sequence

as recited in amended independent claim 78. For at least these reasons, amended independent claims 68, 73, and 78 are patentable over Kawamura and Cheung.

Claims 5-8, 11, 12, 17-21, and 69-72 depend from claim 68. Claims 48, 49, 51, 52, and 74-77 depend from claim 73. Claim 79 depends from claim 78. For at least these reasons, and further in view of their own features, dependent claims 5-8, 11-14, 17-21, 48, 49, 51-54, 69-72, 74-77, and 79 are patentable over the combination of Kawamura and Cheung. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Kawamura, Cheung, and Steinman

Claims 13, 14, 53, and 54 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kawamura and Cheung and further in view of U.S. Patent No. 6,591,349 to Steinman, et al. (Steinman). Applicants respectfully traverse this rejection.

Claims 13 and 14 depend from claim 68 and claims 53 and 54 depend from claim 73. Steinman does not overcome the deficiencies of amended independent claims 68 and 73 described above. For at least these reasons, and further in view of their own features, dependent claims 13, 14, 53, and 54 are patentable over

Kawamura, Cheung, and Steinman. Reconsideration and withdrawal of the rejection are therefore respectfully requested.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon
Attorney for Applicants
Registration No. 50,633

Date: April 3, 2008

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600